Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Digital Broadcast Content Protection Rule Broadcast Flag Certifications	)	___ Docket No. _____

BROADCAST FLAG CERTIFICATION OF TIVO INC.

Matthew Zinn
General Counsel

Max P. Ochoa
Corporate Counsel

TiVo Inc.
2160 Gold Street
P.O. Box 2160
Alviso, CA 95002-2160

James M. Burger
Briana E. Thibeau

Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 776-2300

February 27, 2004

Table of Contents

Page

Table of Contents

Page

Summary

In adopting final rules to implement a flag-based protection system for digital television content, the Federal Communications Commission ("FCC" or "Commission") has established an interim approval process for digital output protection technologies and recording methods. This process permits proponents of a specific digital output protection technology or recording method to seek an FCC determination that such technology or method is appropriate for use in covered demodulator products to give effect to the broadcast flag. It is pursuant to this interim approval process that TiVo Inc. ("TiVo") submits this certification seeking approval of its digital output protection technology.

As a leading provider of television services for digital video recorders ("DVRs"), TiVo offers a subscription-based service with unprecedented media management capabilities. The TiVo® service places control over television viewing in the hands of consumers by allowing them to view preferred programs at any time after they air, and to pause, rewind, and fast forward "live TV." In addition, many TiVo devices also have features that take advantage of the DVR's connection to the television and the home network to add value to consumers' experience of other digital media, such as photos and music. These innovative features, and TiVo's unprecedented focus on the viewer, quickly made TiVo the most popular DVR available in the United States and fueled one of the most rapid adoption rates in the history of consumer electronics. Coupling TiVo's success with digital television ("DTV") will do much to advance the DTV transition.

The most critical factor in TiVo's success, however, is the security of the TiVo system. The strong security of the TiVo system protects TiVo's revenue stream by

giving it the exclusive ability to require payment for provisioning the TiVo service, and to terminate the service in the case of non-payment or piracy. In addition, TiVo's security mechanisms safeguard consumer trust by rigorously protecting the privacy of information that is sent and received by TiVo devices, including anonymous data relating to how customers use their DVRs, as well as information that could be used to identify TiVo customers. Strong security, therefore, is central, and in fact *critical*, to the TiVo business model. Without it, TiVo's revenue stream, the privacy and confidence of its customers, and, ultimately, the continued viability of the company, would be threatened.

Because security is essential to TiVo's business, TiVo designed and implemented an end-to-end security system that is based on a dual-foundation of (i) security in the hardware of TiVo devices, and (ii) security of communications between TiVo devices and the TiVo server. TiVo's digital output protection technology is but one component of this overall system, and the features of the overall system ensure the security of the digital output protection technology. For example, TiVo's security system relies on well understood, well documented, publicly available cryptographic algorithms to establish secure communications with remote TiVo servers and between TiVo devices, and it uses these algorithms to ensure that digital media content and the keys to decrypt it are only sent to other devices in encrypted form. In addition, the TiVo system uniquely associates digital media with a single TiVo device, and only outputs digital media content in individually encrypted clips 5 to 15 minutes in length. As an outgrowth of this overall system, TiVo's digital output protection technology establishes a high standard for the protection of copyrighted material and provides a level of security that is appropriate for use in covered demodulator products, as described in this certification.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Digital Broadcast Content Protection Rule Broadcast Flag Certifications	)	___ Docket No. _____

BROADCAST FLAG CERTIFICATION OF TIVO INC.

Introduction

TiVo Inc. ("TiVo") hereby submits this certification ("Certification") in response to the Federal Communications Commission's ("FCC's" or "Commission's") Final Rule[1] (the "Final Rule" or "Rule") implementing an ATSC flag-based redistribution control system for digital broadcast television content. This Certification is submitted pursuant to Section 73.9008 of the Rule, which establishes an interim approval process for digital output protection technologies and recording methods. Pursuant to Section 73.9008, TiVo seeks approval of its digital output protection technology, and hereby certifies that its digital output protection technology is appropriate for use in covered demodulator products, as set forth herein, to give effect to the broadcast flag.

TiVo's digital output protection technology is but one component of TiVo's overall, end-to-end security system, and the high level of security offered by TiVo's digital output protection technology is an outgrowth of that overall system. Therefore, in

[1] *Digital Broadcast Content Protection, Final Rule*, MB Docket No. 02-230, 68 Fed. Reg. 67599 (released December 3, 2003).

order to understand the level of security offered by the digital output protection technology, it is important to understand the security offered by the overall TiVo system. To establish this foundation of understanding, much of this Certification provides necessary background information about the features of the TiVo® service and the TiVo security system as a whole.

Section I of this Certification provides the Commission with a general overview of TiVo and the TiVo system. Section II provides a description of TiVo's end-to-end security system, which serves as a foundation for the protection of media content introduced into the TiVo system. Finally, Section III of this Certification provides a detailed analysis of TiVo's digital output protection technology, including:

(1) a general description of how TiVo's digital output protection technology works, including its scope of redistribution;

(2) a detailed analysis of the level of protection TiVo's digital output protection technology affords content;

(3) information regarding the licensing of TiVo's security system, including its digital output protection technology; and

(4) a statement certifying that TiVo does not offer its security technology as a free-standing digital output protection or recording technology, and does not intend to do so in the future.

TiVo respectfully requests that the Commission issue a determination indicating that TiVo's digital output protection technology is authorized for use in covered demodulator products.

I. About TiVo

A. The Company and its Philosophy

TiVo is a leading provider of television services for digital video recorders ("DVRs"), a rapidly growing consumer electronics category. The subscription-based full TiVo service provides consumers with a unique entertainment service that offers an easy way to record, watch, and control television. The development of this service springs from TiVo's founding vision to continually innovate and enhance the ways people experience entertainment, from television, to music, to movies and photos. With its first invention – the DVR – TiVo provided consumers with an easy to use service that allows them to enjoy television content in their home at their convenience. The DVR also set a tone for future TiVo efforts that continue its focus on facilitating innovative consumer uses and practices while protecting content. In addition to the value the TiVo service offers consumers, it offers advertisers, content creators, and television networks a new platform for promotions, content delivery, and audience research. Extending these consumer benefits to digital television will do much to advance the DTV transition.

B. The TiVo® Service

TiVo sells the TiVo service, and it designs, manufactures, and licenses manufacturing rights to devices that are dependent on the service for full functionality ("TiVo Devices"). A TiVo Device may be fully specified by TiVo – for example, a TiVo DVR capable of running TiVo application software – or it may be a hardware plug-in (for example, a USB[2] plug-in) that enables TiVo-specified functionality in a software application.

[2] See attached Appendix A for a glossary of technical terms.

The TiVo service is currently available in two tiers. The first tier is a free, basic service with a restricted set of features that is bundled with some DVD devices; the second is the full TiVo service. The second tier is accessed when a consumer purchases either a monthly subscription to the TiVo service, or a "Product Lifetime" subscription that requires a single payment and purchases the service for the functional lifetime of a single device. Because a TiVo Device without the TiVo service generally has little to no functionality, the digital output component on such a device is not enabled.

As a condition for maintaining the TiVo service, a TiVo Device must periodically contact remote servers operated by TiVo and housed at secure facilities. These servers provision TiVo Devices with the up-to-date data required by various features of the service. Devices contact the service using either a standard phone line or an Internet connection.

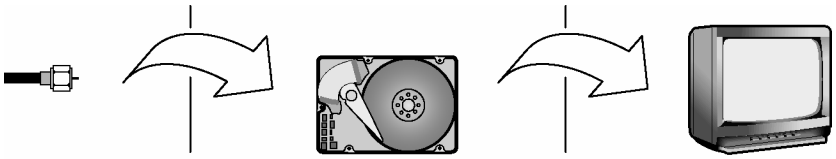
1. Consumer Appeal

TiVo pioneered the DVR category of consumer products, placing a previously unprecedented level of control over the home entertainment experience directly into the hands of its customers. Current models of TiVo Devices also have features that take advantage of the DVR's connection to the television, the home network, and the Internet to add value to consumers' experience of other digital media, such as digital music and digital photos.

a. General Description of How a TiVo® DVR Works

In a home entertainment system, the TiVo DVR fits between an incoming television signal and a television. The DVR intercepts the incoming television signal. If the signal is digital, the DVR will demodulate and decode it, inspect it for the broadcast

flag, encrypt it, and save it to a hard disk; if the signal is analog, the DVR will first digitize it, then encrypt it and save it to a hard disk. As the DVR processes the incoming signal, it creates an alternate media stream for output to the television. The customer actually sees and hears the DVR's alternate media stream.



As the TV signal comes in, the DVR encrypts it and saves it to a hard disk.

The DVR creates an alternate media stream for the TV.

If the customer is watching "live TV," the alternate media stream includes the incoming television signal, only slightly delayed for processing. Because the alternate stream comes from media saved to the hard disk, the customer can pause it, and can rewind and fast forward through the saved portion. This gives the customer an unprecedented level of control over live TV.

A TiVo DVR acquires program information, channel listings, program schedules, and descriptions from the TiVo service. The DVR then applies its computing power to let the consumer sort and search through the data within a straightforward, intuitive user interface. The TiVo DVR owner can easily find programs of interest and schedule the DVR to record them. Over time, a DVR generally builds up a reserve of programming that interests the owner, so the owner always has something appealing to watch. The owner also no longer needs to be concerned with the television schedule. When a desired program airs, the DVR records it and makes it available for viewing at any time thereafter.

b. TiVoToGo

There are currently two kinds of TiVo Devices. The first is the TiVo DVR, described in detail above. The second is a plug-in hardware dongle (for example, a USB dongle) that is registered with the TiVo service. Connecting the hardware dongle to a personal computer on which a TiVo-specified software application has been loaded enables "TiVoToGo" functionality in the software application. The TiVoToGo functionality is only useful to a consumer if:

- He or she has registered the plug-in dongle with TiVo, and
- He or she has at least one TiVo DVR with a subscription to the TiVo service that is registered to the same customer account as the plug-in dongle.

TiVoToGo allows a consumer to copy recorded content between a TiVo DVR and one or more computers equipped with a hardware plug-in dongle that is registered on the same customer account as the DVR. When a registered dongle is plugged into a computer, a consumer can use that computer to view the transferred content. Because the dongle can only be plugged-in to a single computer, even though a registered dongle can enable TiVoToGo functionality on more than one computer, it can only enable one computer at a time to view transferred content. This mechanism effectively inhibits the indiscriminate redistribution of content and, by including a hardware component, provides a level of security that surpasses current industry standards.

By requiring the use of the hardware plug-in dongle, TiVoToGo is able to implement all of the security features of the TiVo digital output protection technology as described in Section III, below.

c. The Advantage to Consumers

In addition to the two capabilities discussed above – control over live TV and effective "time-shifting" (the ability to watch programming at any time after it airs) – the TiVo service also offers many other DVR features, such as the ability to suggest new programs a viewer may like based on the programs he or she has liked in the past. The full suite of DVR features included in the TiVo service offers consumers the most satisfying, easy-to-use DVR experience currently available.

One of the key values of a TiVo DVR is the freedom it imparts from the constraints of programming schedules. This provides TiVo customers with more flexibility in how they manage their time – a value that resonates through many seemingly unrelated areas of their lives. For example, if a household has a TiVo DVR, a child's homework time need never conflict with his or her desire to watch a specific program. No matter when it airs, the program can be available after the child finishes his or her homework. This change in routine can provide an enormous value to harried parents, who also may receive additional benefit by recording their favorite programs and watching them after their children have gone to bed.

Easy recording and playback also adds value to the television service consumers already purchase, expanding the diversity of programs they receive by making every program available to be viewed, no matter when it airs. These are some of the reasons why, in a recent survey, TiVo customers reported a 97% satisfaction rate with their TiVo DVRs.[3]

[3] TiVo November 2003 Customer Satisfaction Survey.

TiVoToGo expands on the initial DVR concept by providing a way for consumers to copy content to their own personal computer, known as "space-shifting." Through the TiVo digital output protection technology, TiVoToGo incorporates this added convenience for consumers into a carefully managed framework for the protection of digital media.

2. Additional Media Management Features

In addition to the TiVo features outlined above, TiVo offers consumers many other media management features, among them digital photos ("Digital Photos"), multi-room viewing ("Multi-Room Viewing"), and digital music ("Digital Music"). These features leverage the DVR's links to the television, the home entertainment system and a home network that connects household computers and the Internet.

The Multi-Room Viewing feature employs the TiVo digital output protection technology to securely copy digital media content from one TiVo Device to another. With this feature, consumers who record a program on the TiVo DVR in one room can transfer it to a TiVo DVR in another room where they want to view it. For example, if a consumer records a program in their living room but decides to watch it in their bedroom, they can copy the program to the TiVo DVR in their bedroom.

Many consumers have collections of digital photos stored on their computers. However, their computers may not be in the most convenient location for viewing the photos. Consumers can use the TiVo DVR's Digital Photos feature to solve this problem. After connecting a DVR to a home network that also includes a computer, the Digital Photos feature provides the consumer with easy-to-use TiVo interfaces to access the photos that are stored on the computer and view those photos on a television screen. The

Digital Photos feature also lets consumers manage photos on the personal computer – where they can easily store, edit and organize images – and display them in the comfort of their living rooms on the television.

The TiVo DVR Digital Music feature offers similar benefits to consumers who have converted their personal CD collections to digital music files or have transferable files they have purchased online. Using the intuitive TiVo interface, consumers can access music stored on their networked computer through their DVR. DVRs often connect to a home entertainment system, so this feature is an ideal way to get digital music from the platform best suited to organizing and storing it (the personal computer) to the platform best suited to playing it (the home entertainment system).

These media management features offer consumers exciting new ways to experience video, photos, and music, making the TiVo system an even more attractive proposition to the consumer.

C. The Importance of Security to the Continued Viability of TiVo

Maintaining the security of the TiVo system is critical to the business interests of TiVo Inc. The primary source of revenue for TiVo is subscription revenue from the full TiVo service. To protect this revenue stream, TiVo must protect its exclusive ability to activate and deactivate the TiVo service on TiVo Devices such as DVRs. Piracy of the TiVo service – the use of the service without authorization or payment – threatens the continued viability of TiVo Inc. in the same way that piracy of cable or satellite services would threaten cable or satellite service providers such as DIRECTV or Comcast. TiVo relies on the comprehensive security of the TiVo system to protect itself against piracy.

A breach to the security of the TiVo system could threaten TiVo's vital business interests and continued viability in other ways as well. TiVo DVRs send and receive information that could be used to identify TiVo customers, as well as anonymous data relating to how customers use their DVRs. Consumer confidence in the security and privacy of this information directly affects TiVo's ability to sell TiVo Devices and the TiVo service. A successful attack on the security of the TiVo system that resulted in compromising this information could cripple consumer confidence and cause serious harm to TiVo's business. As detailed in the white paper on privacy that TiVo supplied to the Federal Trade Commission[4], TiVo uses the strong security of the TiVo system to protect the privacy of its subscribers.

II. TiVo's End-To-End Security System: TiVoGuard

Because security is essential to TiVo's business, TiVo designed and implemented an end-to-end security system known as "TiVoGuard." TiVoGuard protects TiVo's exclusive ability to require payment for provisioning the TiVo service, and to terminate the service in the case of non-payment. TiVoGuard also safeguards consumer trust by rigorously protecting private data. TiVoGuard is an essential component of the TiVo system, and the continued success of TiVoGuard is essential to the continued viability of TiVo Inc.

TiVoGuard starts from a secure foundation and builds a chain of security measures that affect every aspect of the operation of a TiVo Device. Among those measures is the digital output protection technology for which TiVo is seeking approval as an authorized technology. As Section III of this Certification demonstrates, TiVo

[4] See http://a423.g.akamai.net/7/423/1788/654f90409cf538/www.tivo.com/pdfs/ftc_letter.pdf (last visited February 26, 2004).

designed its digital output protection technology, a component of TiVoGuard, to be a high standard for the protection of digital media.

This section of the document begins with a brief explanation of some of the basic security mechanisms used by TiVoGuard, and then provides a list of principles that underlie its design. Finally, it describes several of TiVoGuard's basic features in detail. Because TiVo's digital output protection technology fits into the larger TiVoGuard security framework, this description of TiVoGuard is a necessary prerequisite to the description of TiVo's digital output protection technology, which begins in Section III.

A. Basic Security Mechanisms

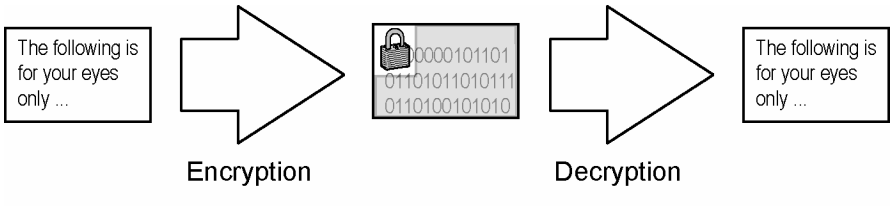
To understand the level of security provided by TiVoGuard, it is useful to understand some of the basic security mechanisms that the system employs. TiVoGuard employs encryption and decryption to protect secrets and protect data from unauthorized use. It also employs digital signing to verify the integrity and authenticity of software and data including communications between multiple TiVo Devices, and communications between individual TiVo Devices and remotely operated TiVo servers.

1. Cryptography

a. Digital Cryptographic Ciphers

TiVo uses digital cryptographic ciphers to protect secrets and to protect data from unauthorized use. Digital cryptographic ciphers encrypt and decrypt data. The purpose of encrypting data is to protect it by rendering it unintelligible. Encryption accomplishes this by scrambling the data according to a set of rules (an "algorithm"). In its encrypted form, the data is protected because it cannot be understood. Decryption is the reverse

process: it starts with encrypted data and applies an algorithm to return the data to its original, unencrypted form.



b. Cryptographic Algorithms and Keys

Digital cryptographic ciphers commonly employ a kind of algorithm that requires a "key." An algorithm of this kind requires two inputs – the data to be encrypted or decrypted, and a key that determines how the algorithm will change the data.

For example, one simple algorithm for encrypting English is: "For each letter from A to Z, replace it with the letter that is N positions to its right in the alphabet. When you get to the end of the alphabet, wrap back to the beginning." The output of this algorithm will change depending on the value of N. If N equals 5, the word "big" becomes "gnl"; if N equals 6, the word "big" becomes "hom."

In the example above, you must select a value for N before encrypting the text. The value you select becomes the encryption key. You use the same value with a related algorithm to decrypt the text, making it the decryption key as well. (In this example, the decryption algorithm uses 'shift to the left' instead of 'shift to the right.')

c. Symmetric and Asymmetric Key Ciphers

Most commonly used digital cryptographic ciphers fall into two broad categories: symmetric key ciphers and asymmetric key ciphers. Symmetric key ciphers use only one cryptographic key – that is, they use the same value for both the encryption key and the decryption key.

If neither the cryptographic cipher nor the decryption key is secret, then encryption provides no security. Modern cryptographic ciphers are generally widely understood. Consequently, for symmetric key ciphers to provide security the key must remain secret. A classic problem for symmetric key ciphers is how to securely distribute the key.

Asymmetric key ciphers use a pair of cryptographic keys. Information encrypted with one key can only be decrypted with the other key. When an asymmetric key cipher generates a pair of keys, one is generally designated as the "public key." This key may be widely distributed and is not considered a secret. The other key is the "private key" and is kept secret. Anyone may encrypt data using the public key, but only those who know the private key can decrypt that data. Asymmetric key ciphers are sometimes referred to as "public-key ciphers."

d. Levels of Protection

Assuming that a symmetric cryptographic cipher's key remains secret, two factors determine the level of security it provides: the strength of the algorithm used and the number of possible keys. The example used in subsection (b), above, is a very weak cipher. If you do not know the decryption key, analyzing it sufficiently to determine the key requires only a trivial effort. In addition, the number of values for N that yield unique results is only 26. This makes it easy to find the decryption key using the "brute force" approach of trying each of the 26 unique keys.

The algorithms used by most modern cryptographic ciphers have not been broken through analysis despite being widely published and understood. This leaves the size of their "key space" – the number of possible keys – as the critical factor determining the

level of protection they provide. The key space is represented by the "key length," usually expressed in bits, such as a "50-bit key length" or a "128-bit key length." Each increment represents a factor of two, so a 51-bit key length has twice as many possible keys as a 50-bit key length. In real terms, a 50-bit key length represents roughly 1.1 x 10^{15} possible keys; a 128-bit key length represents roughly 3.4 x 10^{28} possible keys.

TiVoGuard uses 128-bit keys with all of its symmetric cryptographic ciphers. Although breakthroughs in mathematics and computing are impossible to predict, the best estimates of cryptanalysts suggest that strong symmetric ciphers with keys 128-bits long should be secure against brute force attacks for several decades. Well regarded estimates posit that at the current level of understanding, a brute force attack employing 100 billion dollars of today's computing power would require roughly 10,000,000,000,000 years to break such a cipher.[5]

In the context of the mathematics used to create most asymmetric ciphers, key length has a different significance than it does for symmetric ciphers, and acceptable key lengths must be much longer. TiVoGuard currently uses an El Gamal cipher with an 894-bit key length for asymmetric encryption operations, providing for a different unique key of this length to protect the content of each TiVo Device. Extrapolating from the widely accepted estimates in Bruce Schneier's *Applied Cryptography*[6] and assuming today's understanding of cryptanalytic techniques, a 10 million dollar investment in a brute force attack on one of these keys would break the cipher for a single TiVo Device in roughly 2400 years. The TiVoGuard system further protects critical private keys by

---

[5] Bruce Schneier, Applied Cryptography, 2nd Edition (New York, NY: John Wiley & Sons, Inc., 1996), 153.

[6] *Id.* at 153.

embedding them in cryptographic chips from which they cannot be extracted. The chip performs cryptographic operations very slowly, which further reduces the likelihood of a successful brute-force attack by increasing the time required to iterate through all possible values.

e. Cryptography and TiVoGuard

Because different cryptographic ciphers have different strengths, TiVoGuard's designers built a system that uses different ciphers for different kinds of information. The information TiVoGuard encrypts and decrypts falls into three broad categories:

- Cryptographic keys
- Software files and other data proprietary to the TiVo service
- Digital media

As described in Section II(C)(2), below, the designers of TiVoGuard built mechanisms to renew the system by replacing specific cryptographic ciphers as TiVo deems that advances in cryptanalysis have made it prudent to do so. TiVoGuard currently uses the following ciphers:

- The El Gamal asymmetric cipher with an 894-bit key. As with all asymmetric ciphers, El Gamal requires a public and a private key. It is essential that its private key remain secure. Therefore, the private key is embedded in a special cryptographic chip. While data can be passed through the chip for encryption or decryption, neither TiVo nor anyone else can extract the private key from the chip. In addition, to help protect the chip from brute force attacks, it encrypts and decrypts data very slowly. This cipher provides TiVoGuard with

strong security for small pieces of data. TiVoGuard generally uses the cryptographic chip to encrypt and decrypt other cryptographic keys.

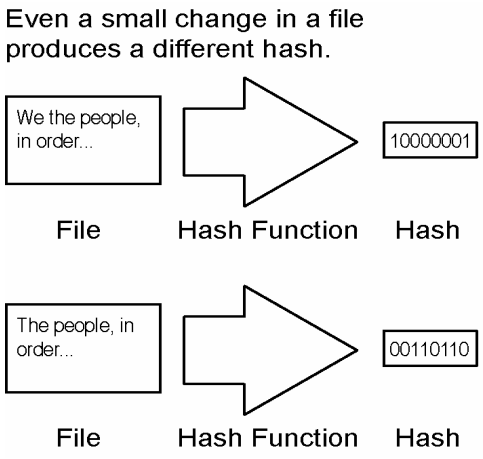
- The Blowfish symmetric cipher with a 128-bit key. Blowfish is a "block cipher," meaning it efficiently encrypts and decrypts data in discrete chunks. TiVoGuard generally uses the Blowfish cipher to encrypt and decrypt software files, some cryptographic keys, and other data proprietary to the TiVo service.
- An "Alternating Stop & Go" Linear-Feedback Shift Register ("LFSR") "stream cipher" with a 128-bit key. Stream ciphers efficiently encrypt and decrypt data streams, such as media streaming from a hard disk to a display. TiVoGuard uses this cipher to encrypt and decrypt digital media.

2. Digital Signing

To ensure the security of communications, the receiver of a communication must be able to verify its authenticity – that it originated with the expected sender – and its integrity – that a third party did not alter it in transit. TiVoGuard addresses these concerns through digital signing.

a. Using a Hash Function to Verify Integrity

To verify the integrity of a file, TiVoGuard uses a "hash function." The purpose of a hash function is to produce a "hash" – a very small, very specific abstract of a file that identifies the file in a manner similar to how a



fingerprint identifies an individual. (A hash is typically a string of ones and zeros.)

The likelihood of two different files yielding the same hash is statistically insignificant. TiVoGuard can verify a file's integrity by comparing a hash produced from a trusted copy of the file with a hash produced from the file in its current state. If the two hashes match then the current file has the same content as the trusted copy, and its integrity is verified. TiVoGuard currently uses the SHA-1 hash function, an algorithm published by the National Security Administration ("NSA") as a Federal Information Processing Standard ("FIPS"). SHA-1 is currently in wide use and has suffered no known successful cryptanalytic attacks.

b. Using an Asymmetric Cipher to Verify Authenticity

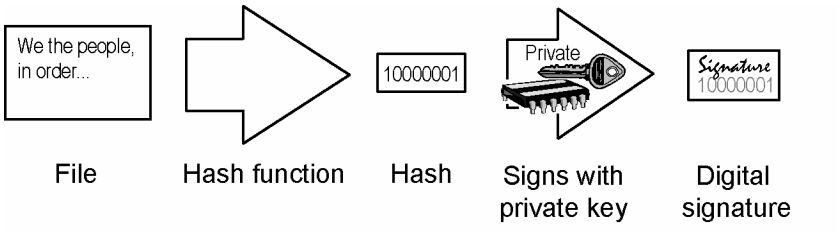
In addition to verifying the integrity of a file, a secure system must also consider the authenticity of a file. If an attacker tampered with the file, he or she might also have tampered with the hash of the trusted copy of the file – substituting a hash of an altered file. To provide true security, the system must either store the hash of the original file in a tamper-resistant location, or be able to verify its authenticity.

TiVoGuard uses an El Gamal public and private key pair to verify the authenticity of hashes. First, TiVoGuard uses a private key to "sign" the hash. The TiVo Device then uses the corresponding public key to verify that the private key created the signature. Because private keys are secret, verifying that a hash was signed by a specific private key verifies the authenticity of the hash. The 894-bit key length TiVoGuard uses for digital signatures falls within the 512- to 1024-bit requirements for the Digital Signature Standard ("DSS") provided by the NSA for use with the Digital Signature Algorithm ("DSA"), a related signature algorithm.

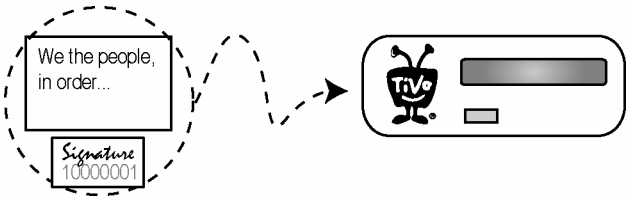
c. The TiVoGuard Digital Signature

A TiVoGuard digital signature is a hash signed by a private key. The following example shows how TiVoGuard uses a digital signature to verify the authenticity and integrity of a communication from the TiVo service to a TiVo Device.

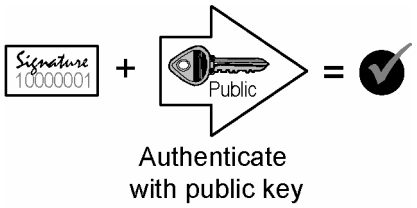
1. The TiVo service creates a digital signature for the communication.



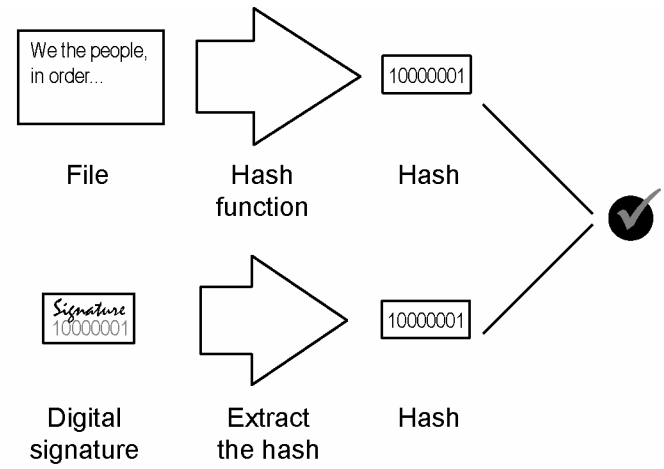
2. The TiVo service then sends the signature and the communication to a TiVo Device.



3. To verify the authenticity of the communication, the TiVo Device uses the corresponding public key to determine whether or not the correct private key signed the hash.



4. The TiVo Device calculates a new hash from the file, then extracts the hash from the digital signature. If the calculated hash matches the hash from the signature, then the file has not changed since it was sent.



B. Design Principles

In designing TiVoGuard, TiVo engineers started from the following short list of basic principles:

- Use well understood, well documented, publicly available cryptographic algorithms whose security has withstood public scrutiny, including that of the cryptographic community.
- Eschew "security through obscurity." Do not use algorithms that might be compromised by becoming known.
- Eschew global secrets. Design so that defeat of any one component of the system compromises as little as possible.
- Build for the future. Provide for renewability, upgradeability, and revocability.

- Be informed and responsive. Continuously monitor and respond to security developments in general, and security developments that affect the TiVo system in particular.

C. The Dual Foundation of TiVoGuard

TiVoGuard is based on the dual foundation of: (i) security in the hardware of TiVo consumer devices; and (ii) establishing secure communications with the TiVo servers that provides a channel for feature upgrades, renewability, and revocability.

1. Security in the Hardware of TiVo Consumer Devices

In individual TiVo Devices, TiVoGuard begins with a cryptographic chip that provides tamper-resistant security in hardware. The data and routines in the cryptographic chip cannot be altered. The cryptographic chip provides the following three basic functions:

- It generates an asymmetric public and private key pair and keeps the private key secret. After generating the private key, the chip disables all circuits through which the private key might be accessed. While the public key remains accessible and can be extracted from the chip, the private key cannot be accessed in any way; it can only be used by the cryptographic chip.
- It uses the private key to decrypt and encrypt data.
- It uses the private key to create digital signatures.

The cryptographic chip creates a foundation upon which TiVoGuard builds secure content storage (as described in Section II(D), below) and the TiVoGuard digital output protection technology (as described in Section III, below).

2. Renewability, Revocability, and Feature Upgrades Through Secure Communication with the TiVo Servers

TiVoGuard includes mechanisms that allow TiVo Devices to establish secure communications with TiVo servers. TiVo Devices regularly communicate with TiVo servers at remote facilities to acquire program information, data updates, and/or software updates, and to upload data. Through software updates, TiVo can add new features that enhance the value of the TiVo service. Software and data updates also allow TiVo to revoke the features of the TiVo application that allow output and reception of digital media content. In addition, the updates give TiVo the ability to modify or renew security mechanisms, such as specific cryptographic ciphers, as TiVo deems it necessary or prudent to do so (*e.g.*, in the event of a system compromise or advances in cryptanalysis). Because TiVo's success as a business depends on the security of its system, any different security mechanism employed by TiVo in the future will be sufficiently strong so as not to materially compromise the security of the system.

To establish secure communications, TiVoGuard relies on an exchange of public keys between the TiVo servers and TiVo Devices. As described in Section II(A)(2), above, this exchange allows private keys to be used to create digital signatures. The corresponding public keys can then be used to validate the authenticity of those signatures.

a. Provisioning Devices with Server Public Keys

To provision TiVo Devices with the public keys from TiVo servers, TiVo embeds the keys in application software. When a device runs the software, it has access to the servers' public keys. Embedding is an important component of the security framework in application software or in media and is a standard technique employed by the most

widely used Digital Rights Management ("DRM") systems. For example, many DRM systems embed a critical URL in each file that contains encrypted digital media. Before decrypting the media, a compliant player uses the URL to locate an online certificate that confirms the individual consumer's right to view the media. A third party (other than the DRM licensor or the owner of the media copyright) often administers the online certificates. In contrast, by embedding the service public key in the software, TiVoGuard eliminates the need to rely on a third party and allows TiVo to directly manage all of TiVoGuard's cryptographic keys. Both of these points are important strengths of the TiVoGuard system that TiVo relies on to protect its vital business interests.

b. Provisioning Servers with Device Public Keys

To provision the TiVo servers with a unique public key for each TiVo Device, TiVoGuard uses a unique manufacturing process. The process is used on any TiVo Device that contains a cryptographic chip such as the one described in Section II(C)(1) (currently TiVo DVRs and the TiVoToGo USB plug-in dongle). When the device first powers on during manufacturing, the cryptographic chip generates an El Gamal public/private key pair with an 894-bit key length. TiVoGuard's manufacturing module captures the public key, pairs it with a unique identifier for that device, and sends both items over a secure channel to the TiVo servers. The TiVo servers maintain a log of all TiVo Devices and their corresponding public keys. TiVo does not recognize any devices not made under the authorization of TiVo.

D. TiVoGuard Content Storage

TiVoGuard effectively and uniquely associates all digital media content with a single TiVo Device – whether the device is a TiVo DVR or a TiVoToGo USB dongle.

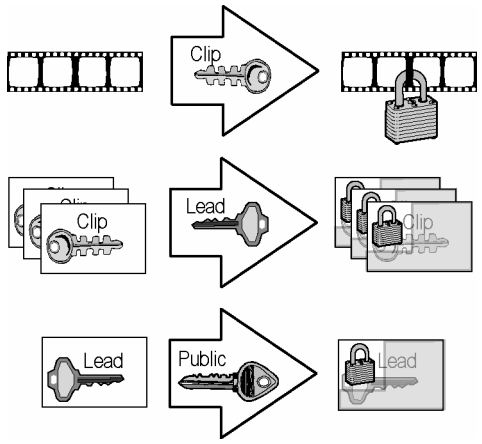
TiVoGuard generates a "lead encryption key" the first time a TiVo Device powers on. The lead encryption key is used to decrypt and encrypt other encryption keys. Currently, TiVoGuard uses a 128-bit key for the Blowfish cryptographic cipher as the lead key.

As digital media enters the TiVo system, the system divides it into media clips of from five to fifteen minutes in length (depending upon the recording quality selected for that program). For each clip, TiVoGuard generates a unique 128-bit key for the Alternating Stop & Go LFSR stream cipher. It uses this "clip key" to encrypt the clip. It also uses the lead key to encrypt each clip key, and uses the device's public key to encrypt the lead key. Through these cryptographic processes (summarized below), TiVoGuard uniquely and effectively associates each clip with a single TiVo Device.

1. Clip Encryption

To encrypt clips, the system:

- generates clip keys and uses them to encrypt the digital media clips; then
- uses the lead key to encrypt the clip keys; then
- uses the device's public key to encrypt the lead key.

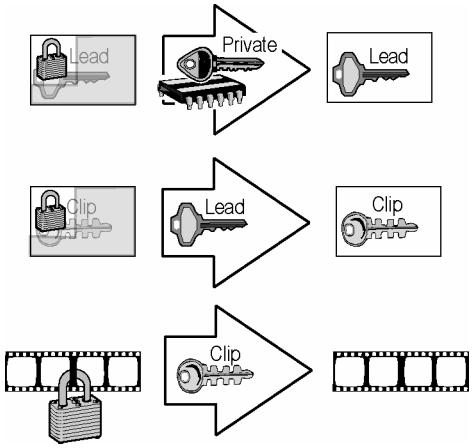


The system saves only encrypted clips and encrypted cryptographic keys to a device's hard disk.

2. Clip Decryption

To decrypt a clip, the system must first:

- use the device's private key to decrypt the lead key; then
- use the lead key to decrypt the clip key; then
- use the clip key to decrypt the clip.



A clip cannot be decrypted without the device's private key, which only exists in the device's cryptographic chip. Each clip is therefore uniquely and effectively associated with a single device.

III. TiVoGuard Digital Output Protection Technology

The TiVoGuard security system starts from the secure foundation described in Section II and builds a chain of security measures that affect every aspect of the operation of a TiVo Device, including its digital output. By making its digital output protection technology a part of the TiVoGuard end-to-end security system, TiVo designed its digital output protection technology to provide a high standard for the protection of digital media.

To demonstrate that its digital output protection technology is appropriate for use in covered demodulator products to give effect to the broadcast flag, TiVo provides in this Section III a detailed analysis of its digital output protection technology, including: (1) a general description of how TiVo's digital output protection technology works, including its scope of redistribution; (2) a detailed analysis of the level of protection TiVo's digital output protection technology affords content; (3) information regarding the

licensing of TiVo's security system, including its digital output protection technology; and (4) a statement certifying that TiVo does not offer its security technology as a free-standing digital output protection or recording technology, and does not intend to do so in the future.

A. General Description of TiVo's Digital Output Protection Technology

TiVoGuard includes digital output protection technology that a TiVo Device can use to send digital media content to another TiVo Device. To use this technology, the two devices must be in the same "secure viewing group." A secure viewing group is a collection of TiVo Devices that meet criteria specified by TiVo and that have been associated by a TiVo customer. Content cannot be copied from one TiVo Device to another device that is not in the same secure viewing group.

1. Establishing a Secure Viewing Group

Only a TiVo Device that meets all of the following criteria may be placed with other devices in a secure viewing group:

- Every TiVo Device must be registered with the TiVo service and only devices registered on the same customer account may be in the same secure viewing group. For example, an individual who has registered two TiVo DVRs and a single TiVoToGo USB dongle may put all three devices in the same secure viewing group.
- The device can be in only one secure viewing group.
- TiVo policy currently prevents customers from creating secure viewing groups with more than 10 TiVo Devices. In exceptional circumstances, TiVo may create a secure viewing group that includes up to 20 devices.

Customers may place TiVo Devices that meet these criteria into a secure viewing group via a password protected web interface or by calling TiVo customer support. By restricting the number and nature of the TiVo Devices that can be placed in a secure viewing group, the TiVo system restricts the scope of redistribution for the TiVoGuard digital output protection technology.

2. The TiVoGuard Certificate

When a TiVo Device contacts the remote TiVo servers, the servers may send it a "TiVoGuard certificate." If the device is part of a secure viewing group, the TiVoGuard certificate lists every device in that group. For each device in the group, the certificate includes a unique identifier and the device's public cryptographic key. Because every TiVo Device has access to the public keys for the TiVo service (see Section II(C)(2), above), the TiVo service can sign the TiVoGuard certificate, allowing the receiving device to verify the certificate's authenticity and integrity.

TiVoGuard certificates also include an expiration date. In standard operation, each device routinely contacts the TiVo service, which in turn regularly renews TiVoGuard certificates, extending their expiration dates. However, if a customer operates a TiVo Device in a manner that does not allow contact with a TiVo server, the TiVoGuard certificate expires and the device loses its ability to send content to another device. TiVoGuard certificates can also be revoked by the TiVo Service during a DVR's regular communication with the service.

3. Establishing a Secure Channel for Communications Between TiVo Devices

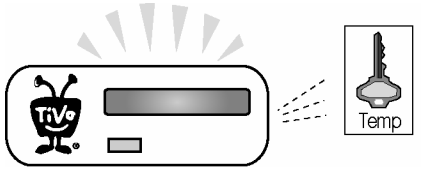
Two networked TiVo Devices in the same secure viewing group may discover each other using a standard TCP/IP protocol. Each will have a TiVoGuard certificate that

includes the public cryptographic key of all of the TiVo Devices in that viewing group. This allows the two devices to use each other's public keys to establish a secure channel on the network by encrypting and digitally signing communications.

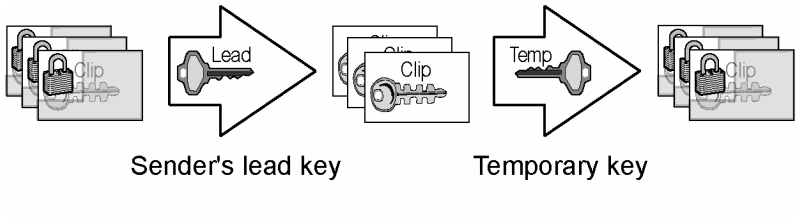
4. Sending Digital Media Content

TiVoGuard protects digital media content as it transmits the content from one TiVo Device (the "sender") to another (the "receiver") as follows.

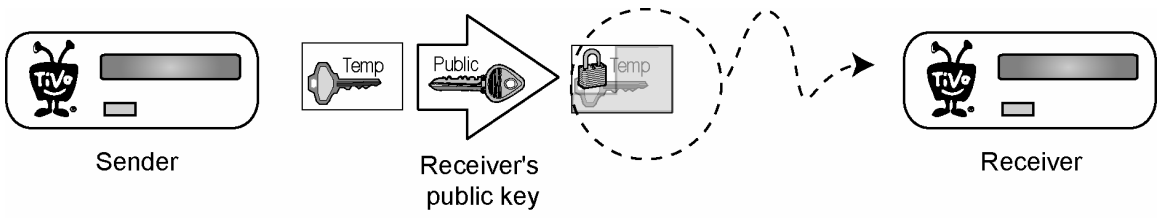
1. The sender generates a unique, temporary encryption key (like the lead key, the temporary key is a 128-bit Blowfish key).



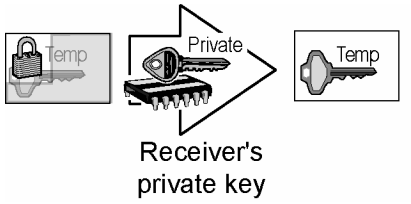
2. The sender uses its own lead key to decrypt the clip keys for content it will send, and then the sender re-encrypts the clips with the temporary key.



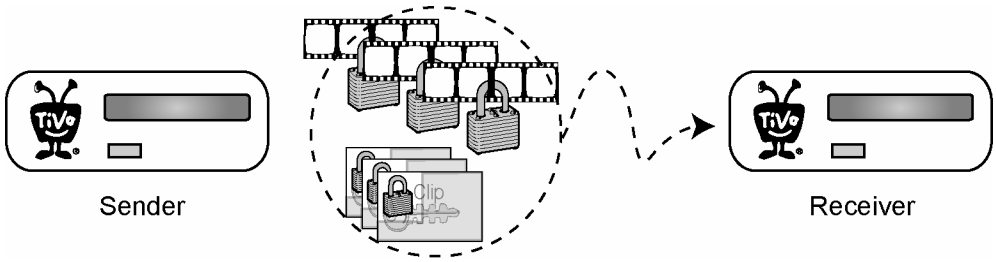
3. The sender uses the receiver's public key to encrypt the temporary key and then sends it to the receiver.



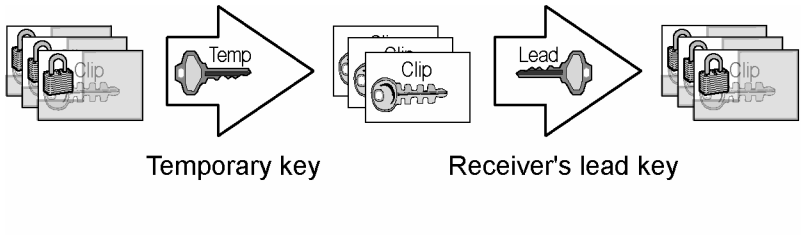
4. The receiver uses its cryptographic chip to decrypt the temporary key.



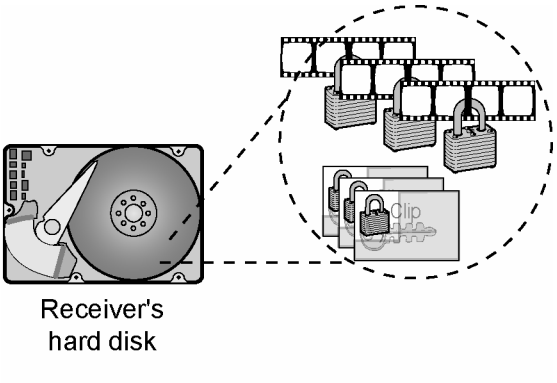
5. The sender sends the encrypted clip keys and encrypted clips to the receiver. No content or clips are ever sent in the clear.



6. The receiver uses the temporary key to decrypt the clip keys transmitted by the sender, and then uses its own lead key to re-encrypt them. In this way, the content stored on the receiver is uniquely associated with that device so that such recording cannot be accessed in usable form by another product except by TiVo's digital output protection technology, or, in the future, by another Authorized Digital Output Protection Technology.



7. The receiver can now store the encrypted clips and encrypted clip keys on its hard disk.



This digital output protection technology accommodates consumers' use and enjoyment of unencrypted digital terrestrial broadcast content and facilitates the transition to digital television. By allowing consumers to exchange content only within a secure viewing group, TiVo provides content owners more than "reasonable assurance that DTV broadcast content will not be indiscriminately redistributed while protecting consumers' use and enjoyment of broadcast video programming."[7]

B. Detailed Analysis of the Level of Protection the TiVoGuard Digital Output Protection Technology Affords Content

1. Level of Security

Based on secure communications with remote TiVo servers, and combinations of strong cryptographic ciphers employing proven algorithms (with key lengths of 128-bits for symmetric ciphers and 894-bits for asymmetric ciphers), the TiVoGuard digital output protection technology provides an overall level of security that establishes a high standard for the protection of copyrighted material. As described in this Certification, the

[7] *Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rule Making,* MB Docket No. 02-230 (rel. Nov. 4, 2003) at ¶ 4.

TiVoGuard security system has numerous features that ensure the security of TiVo's digital output protection technology, including the following:

- TiVoGuard cryptographic measures allow TiVo Devices to establish a secure channel for communications with other TiVo Devices and with remotely operated TiVo servers.
- Digital media content and the keys to decrypt it are only sent to other devices in encrypted form. No content or keys are sent unencrypted.
- Unencrypted digital media content and unencrypted cryptographic keys only exist within TiVo Devices as Transitory Images (as defined in Section 73.9000(o) of the Rule) and are not available on user accessible buses.
- TiVoGuard outputs digital media content in individually encrypted clips 5 to 15 minutes in length, so a successful cryptographic attack is likely to compromise very little content.
- While digital media is being sent, TiVoGuard effectively and uniquely associates it with only the TiVo Device sending it and the TiVo Device receiving it.

2. Authentication

As described in Section III(A), above, the TiVoGuard certificate provides all devices in a secure viewing group with the public keys of other devices in the same group. As a result, communications between TiVo Devices can be authenticated and their integrity verified.

3. Scope of Redistribution

The scope of redistribution is limited by the fact that both the sending and the receiving device must be in the same secure viewing group. As described in Section III(A)(1), above, all devices in a secure viewing group must meet specific criteria established and maintained by TiVo.

4. Upgradeability and Renewability

As discussed in Section II(C)(2), above, the TiVoGuard digital output protection technology is upgradeable and renewable via secure software and data updates from remotely operated TiVo servers. While these updates allow TiVo to renew security mechanisms, such as specific cryptographic ciphers, as well as add or revoke features of the TiVo application, TiVo will not – and its business model demands that it not – make any changes to the TiVo system that would materially compromise the security of the system. In the event that TiVo deems it necessary or prudent to modify or renew its security mechanisms (*e.g.*, in the event of a system compromise or advances in cryptanalysis), TiVo will notify the Commission of the different security mechanism(s) employed and will ensure that any such changes are made within the framework of the Rule.

5. Interoperability

TiVo Devices may only use the TiVoGuard digital output protection technology to send digital content to other devices that implement the TiVoGuard system.

6. Revocability of Compromised Devices

By altering a device's TiVoGuard certificate during a secure communication with the TiVo servers, the TiVo service may revoke the features of the TiVo application that

allow output and reception of digital media content. The TiVo service is capable of revoking such features for specific, individual TiVo Devices, or for groups of TiVo Devices.

If a TiVo Device does not regularly contact TiVo servers, the features that allow output and reception of digital media content are automatically revoked through the expiration of the device's TiVoGuard certificate.

C. Information Regarding the Licensing of TiVoGuard Technology

1. Licenses Granted to Select Equipment Manufacturers

TiVo's licensing strategy promotes the mass development of consumer electronics platforms capable of running the TiVo service. TiVoGuard is part of the TiVo service and includes the TiVoGuard digital output protection technology. In pursuit of its licensing strategy, TiVo has granted licenses to the following leading technology companies that create products providing DVR capabilities:

- Pioneer Corporation
- Toshiba Corporation
- Toshiba America Consumer Products, Inc.
- Sony Electronics Inc.
- Humax Corporation, Limited.
- DIRECTV, Inc.

2. Scope of Licenses

TiVo has not yet licensed the TiVoToGo technology to any equipment manufacturer. For TiVo Devices such as TiVo DVRs for which TiVo specifies the hardware and software, licensees are only authorized to manufacture devices capable of

running the TiVo service in accordance with the thorough hardware and software specifications provided by TiVo. TiVo designed these specifications to allow the full functioning of the TiVo service, including TiVoGuard technology with the security features described in this Certification. Licensees may, at their discretion, include in their final product other digital output protection technologies that have been approved by the Commission.

Among the hardware specifications are detailed requirements for the cryptographic chip, including instructions and schematics relating to installation. TiVo also designs, implements, tests and approves the TiVo software application that provides the TiVo service. During manufacturing, TiVo generally provisions the manufacturer with hard drives preloaded with the TiVo software application. In addition, as devices are manufactured, a module of the TiVoGuard system contacts the TiVo service to upload an inventory of unique identifiers for each device and their associated public keys.

3. Licenses Do Not Threaten the Integrity or Security of the TiVo Service

Licensees do not have the legal authority within the scope of the license to vary hardware construction from specifications provided by TiVo. The TiVo software requires that the hardware that executes it be built to TiVo's specifications. If a licensee does not adhere to the specifications provided by TiVo, the licensee's hardware will not run the TiVo software application or deliver the TiVo service, including the TiVo digital output component. In this way, TiVo Inc. maintains the integrity and security of the TiVo service and thereby protects its vital business interests.

Were a licensee to fail to adhere to the strict TiVo specifications requiring the full implementation of the TiVoGuard security system, that licensee would be in breach of its

license. Moreover, if such a demodulator product used a digital output other than an approved digital output, it would also, in all likelihood, be manufacturing an unauthorized device and be violating the Rule.

D. TiVo's Digital Output Protection Technology is Not Publicly Offered

TiVo does not offer TiVoGuard or the digital output protection component as a free-standing digital output protection or recording technology, and does not intend to do so in the future.

IV. Conclusion

As set forth above, TiVo certifies that its digital output protection technology is appropriate for use in covered demodulator products to give effect to the broadcast flag. Based on the information provided in this Certification, including the attached Appendices, TiVo respectfully requests that the Commission issue a determination, pursuant to Section 73.9008 of the Commission's Final Rule, indicating that TiVo's digital output protection technology is authorized for use in covered demodulator products as requested above.

Respectfully submitted,

TIVO INC.

/s/ James M. Burger

James M. Burger
Briana E. Thibeau
Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 776-2300

Its Attorneys

Matthew Zinn
General Counsel
Max P. Ochoa
Corporate Counsel

TiVo Inc.
2160 Gold Street
P.O. Box 2160
Alviso, CA 95002-2160

February 27, 2004

Appendix A

Glossary

Algorithm
A finite set of rules that gives a sequence of operations for solving a specific type of problem, such as a mathematical formula or the instructions in a program.

Alternating Stop & Go Linear-Feedback Shift Register ("LFSR") Stream Cipher
One of several varieties of possible LFSR stream ciphers whose history extends to the work of Ernst Selmer in the mid 1960s, the Alternating Stop & Go LFSR stream cipher is a publicly available algorithm described on page 383, and visually in Fig. 16.10, of Bruce Schneier's *Applied Cryptography*, 2nd ed. 1996.

Asymmetric Key Cipher
A cryptographic cipher that uses a pair of keys. Information encrypted with one key can only be decrypted with the other key. When an asymmetric key cipher generates a pair of keys, one is generally designated as the "public key." This key may be widely distributed and is not considered a secret. The other key is the "private key" and is kept secret. Anyone may encrypt data using the public key, but only those who know the private key can decrypt that data. Asymmetric key ciphers are sometimes referred to as "public-key ciphers."

Authentication
A process, complementary to encryption in many content protection technology architectures by which the receiver of a message can verify the identity of the message's sender.

Block Cipher
A cryptographic cipher that efficiently encrypts and decrypts data in discrete chunks, or blocks. (The blocks are typically 64-bits long, but may be longer or shorter.)

Blowfish
An unpatented symmetric cryptographic stream cipher designed by Bruce Schneier in 1993.

Broadcast Flag
In the U.S., the Redistribution Control descriptor specified in ATSC Standard A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable, 18 March 2003.

Bus
A transmission path on which signals are dropped off or picked up at attached devices or components.

Cipher
(alt. cryptographic algorithm) A mathematical function or set of related mathematical functions used for encryption and decryption. (There are typically two related functions, one for encryption and the other for decryption.)

Content
Video, audio, subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts, associated data and information, or any other information which may be governed by usage rights.

Cryptanalysis
The art and science of decrypting encrypted data without initially knowing the decryption algorithm and/or the decryption key.

Cryptographic Algorithm
See Cipher.

Cryptographic Chip
Used in this document to refer to a silicon chip incorporated in the design of TiVo Devices. The cryptographic chip produces a unique public/private key pair for the device and maintains the secrecy of the private key. It can also use the public/private key pair to perform encryption, decryption, and digital signing operations.

Cryptography
The art and science of keeping data secure.

Decryption
The process of transforming data from a form in which it is not readily useful into a form in which it is. Decryption is the inverse of Encryption.

Demodulator
A process used to extract baseband digital or analog signals from a radio frequency carrier following reception by a tuner.

Digital Broadcast TV
Over the air, terrestrial broadcast that is transmitted as a digital signal (zeros and ones). The older broadcast TV signal is analog.

Digital Signature
Used in this document to refer to a hash that has been signed by a private key. Signing the hash with a private key allows the receiver to verify the authenticity of the hash. Matching the sent hash with a hash derived from the data file allows the sender to verify the integrity and authenticity of the data file.

DRM
Digital Rights Management. Technology developed by various companies in the IT industry (e.g., Microsoft, RealNetworks, InterTrust) to reveal digital content based upon an arbitrarily developed set of business rules. The highly granular (business) usage rules to be associated with the applicable content, are separate from the content itself, and also from the protection mechanism.

DSA
Digital Signature Algorithm. Published in 1994 by the National Institute of Standards and Technology (NIST) in cooperation with the National Security Agency (NSA) as part of the Digital Signature Standard (DSS).

DSS
Digital Security Standard. Published in 1994 by the National Institute of Standards and Technology (NIST) in cooperation with the National Security Agency (NSA) to be the digital authentication standard of the U.S. Government.

DVR
Digital Video Recorder. A consumer electronics device or a software program that records television programs to a hard drive.

El Gamal
An asymmetric key cipher based on discrete logarithms. Developed by Taher ElGamal in 1984, the ElGamal cipher can be used for encryption, decryption, and digital signing.

Encryption
The process of transforming data from a form in which it can be readily used into a form from which it must be decrypted before being used. The purpose of encryption is to keep data hidden from anyone for whom it is not intended. Encryption is the inverse of decryption.

Hash
(alt. message digest) The result obtained by processing a digital file with a hash function. The hash component of a digital signature can be used to verify the integrity of a file.

Hash Function
A function that takes a variable length input and converts it to a specific fixed length output, or hash. A hash function with practical cryptographic applications typically produces an output that is significantly shorter than the input. The likelihood of two files producing the same output from such a function must be practically insignificant, thereby allowing the hash (the output of the hash function) to identify the original file in a manner analogous to how a fingerprint identifies an individual.

Integrity
The quality of not having been altered or tampered with.

Key Length
Denotes the size of numbers that may be used as cryptographic keys, usually expressed as bits. The key space, or number of possible keys, increases as a function of the key length. A single increment in the key length doubles the field of numbers from which keys may be selected. For typical symmetric ciphers, for which any number expressible within the limits of the key length may be a key, a single increment doubles the key space. Therefore, a 52-bit key length provides twice as many possible keys as a 51-bit key length. For ciphers based on mathematical functions with a more limited key space, such as asymmetric ciphers based on discrete logarithms (e.g., the ElGamal cipher), fewer possible keys are added with each additional increment in the key length.

Key
An input used by a cryptographic cipher to determine how the data on which the cipher operates will be transformed. Modern cryptographic ciphers generally use a numeric key.

Key Space
The number of possible keys available for a specific implementation of a cryptographic cipher. The key space is determined by the key length and the cipher being used.

Linear-Feedback Shift Register ("LFSR")
Most practical stream ciphers are designed around Linear Feedback Shift Registers (LFSRs), an efficient structure for producing numeric sequences that is often also used in random number generation. The Alternating Stop & Go LFSR stream cipher, a publicly available algorithm with a long period and large linear complexity that uses three LFSRs of different length, is described on page 383, and visually in Fig. 16.10, of Bruce Schneier's Applied Cryptography, 2nd ed. 1996.

Modulator
A process used to imprint baseband digital or analog signals onto a radio frequency carrier prior to transmission.

Private Key
A cryptographic key that must remain secret to protect encrypted data. Often used to refer to one key of a public/private key pair generated by an asymmetric key cryptographic cipher.

Product Lifetime Service
A subscription to the TiVo service that covers the life of a TiVo Device such as a TiVo Digital Video Recorder (DVR).

Public Key
One key of a public/private key pair generated by an asymmetric key cryptographic cipher. The public key must be distributed if it is to be used to verify the authenticity of signatures created by the private key. Data encrypted by the public key can only be decrypted by the private key, which remains secret.

Renewability
The ability of a security system to recover from a successful attack and restore protection of the content.

Revocability
The removal of content access or usage privileges previously granted by a rights owner.

Secure Viewing Group
A collection of TiVo Devices that meet criteria specified by TiVo and that have been associated in a group by a TiVo customer.

SHA-1
Published in 1994 as a revision to the Secure Hash Algorithm (SHA), SHA-1 is a hash function published by the National Security Administration ("NSA") as a Federal Information Processing Standard ("FIPS"). When data of any length less than 2^{64} bits is input, SHA-1 produces a 160 bit output (referred to in this document as a hash; also sometimes called a message digest, or fingerprint).

Stream Cipher
Efficiently encrypts or decrypts data streams, such as media streaming from a hard disk to a display, one bit or one byte at a time (depending on the cipher).

Symmetric Key Cipher
A cryptographic cipher that uses the same key for both encryption and decryption.

TiVo Device
A device dependent on the TiVo service for full functionality. A TiVo Device may be fully specified by TiVo – for example, a TiVo DVR capable of running TiVo application software – or it may be a hardware plug-in (for example, a USB plug-in) that enables TiVo-specified functionality in a software application.

TiVo Service
A subscription service that provides functionality to TiVo devices such as TiVo digital video recorders (DVRs).

TiVoGuard
An end-to-end security system implemented by TiVo to provide protection for everything from communication between TiVo devices and remotely operated TiVo servers to any copyrighted content that enters the TiVo system. TiVoGuard defends TiVo's exclusive ability to require payment for provisioning the TiVo service, and to terminate the service in the case of non-payment. TiVoGuard also safeguards consumer trust by rigorously protecting private data.

TiVoGuard Certificate
A certificate provided by the TiVo service to a TiVo device, the TiVoGuard certificate lists all other devices in that device's secure viewing group, as well as properties such as each device's public cryptographic key.

TiVoToGo
A feature of the TiVo service enabled by registration of a hardware plug-in dongle. TiVoToGo allows a consumer to copy recorded content between a TiVo DVR and one or more computers equipped with a hardware dongle registered on the same customer account as the DVR.

USB
Universal Serial Bus. Proposed in March, 1995, by Microsoft, Compaq, DEC, IBM, Intel, NEC, and Northern Telecom as an "open and freely licensable" serial bus, USB a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to a computer without having to add an adapter card or having to turn the computer off.

User Accessible Bus
A data bus designed for end user upgrades or access such as PCI, PCMCIA, or Cardbus, but not memory buses, CPU buses, and similar portions of a device's internal architecture.